Adaptacyjny dostęp do aplikacji wszędzie i z każdego urządzenia
F5 EMEA Webinar Listopad 2014

Andrzej Kroczek
Field Systems Engineer
Today’s Network and App Access: So Many Variables!

LOCATIONS
- Headquarters
- Branch
- Mobile
- Storefront
- Home
- Other Location(s)

USERS
- Mobile Employee
- Contractor
- Remote Employee
- Partner
- Office Employee
- Customer
- Guest
- Other User(s)

DEVICES
- Desktop
- Laptop
- Smartphone
- Tablet
- Wearable
- Camera
- Other Device(s)

APPS & LOCATIONS
- Physical Hosted App
- Cloud Hosted Apps
- Hybrid Cloud Hosted Apps
- Web-based Apps
- Mobile Apps
- Other Apps
- Internet
Mobility is Exploding

THE NUMBER OF MOBILE WORKERS IN WESTERN EUROPE IS EXPECTED TO REACH 512 MILLION BY 2015

*Source: IDC*
Access Management Trends

- Standalone SSL VPN market is static
- Integrated security device market increases – including remote/mobile access
- Remote access plays a vital role in mobile VPN access
Business Challenge: Managing Access Today

- Rapidly expanding, changing mobile workforce
- Explosion in number of users, use cases, in-use devices
- Increased virtualization
- Fast rising number of security threats and attacks

Need to manage access based on identity and context
What is Needed to Control and Manage Access

- Control access based on granular context-based attributes
- Differentiate authentication based on context or emerging methods
- Unify, consolidate, and simplify secure access to all applications
- Provide fast authentication, SSO, and identity federation across applications
- Provide simple user experience for authentication, authorization and access
Control Through Context

User/Device Information + Network/Connection + Application Health & Risk
User Context in Security

Device type and integrity
Operating system
Browser
Location
Intelligence and visibility
Network/Connection Context in Security

- Authentication
- Access method
- Network integrity
- Network quality and availability
- Connection integrity
Application Context in Security
Challenge of Enabling Secure Mobile/Remote Access from Any Device, Anywhere

- Provide full or differentiated network access for employees
- Provide per app access from BYOD or mobile devices
- Provide restricted access for partners and guests
Secure, Accelerated Mobile and Remote Access

- Fast and secure connections maximise productivity for global users
- Seamless integration minimises cost and simplifies end user experience
Multifactor Authentication

User = HR

www.f5.com

HR

AAA Server

© F5 Networks, Inc.
• Ensure integrity and compliance with organizational and regulatory policies regardless of the type of endpoint and OS being used
Difficulty in Sharing Identification Across Any Application, Anywhere

- Silos of identity
- Identity still on-premise but apps and data moving to the cloud
- Too many different passwords needed for multiple different applications
Single Sign-On (SSO) Challenges

- Not all tokens work across all domains
- Some SSO tools must check in with an authorizing decision point
- Difficult to visualise SSO topology and deployment
SSO and Identity Federation Require Greater Flexibility

- Not all applications and identity directories are created equal
- Reworking identifiers sometimes necessary to compensate for legacy applications
- Step-up authentication can’t be used without having a flexible way to assess what credentials are needed and when
Adaptive Authentication and Access

- Transform one type of authentication into another so an application may understand and use it without installing additional agents
- Allow flexible selection of SSO technique appropriate to the application
- Allow for centralized session control of all applications, even SaaS
Identity Federation and SSO Benefits

- Provide seamless access to all resources, including web- and cloud-based apps
- Enhance and simplify the user experience, increase user productivity
- Instantly provision and de-provision access to cloud apps
Identity Federation Architecture
Controlling Enterprise Mobile Access and Managing Enterprise Mobility

- App Wrapping + App Management + Reporting
- Data Center Application Access Management
- Salesforce.com
- Email
- Mobile Application

No data transfer

Data transfer

Managed Apps

Unmanaged Apps
Securing and Managing Mobile Access, Apps, and Devices

Deliver enhanced capabilities over existing mobile access gateways:

- Per app VPN
- Secure remote (SSL VPN) access
- ActiveSync and other proxy services support
- Granular access policy management
- Application access management
- Federated identity/SSO

Integrate with existing market-leading MDM/EMM offerings, seamlessly provisioning mobile devices:

- Mobile application management (MAM)
- Mobile device management (MDM)
- Mobile content management (MCM)
- Sandboxing
- Workspace applications
- File readers and editors
- File systems and portal access
- App wrapping
- Certificate and app provisioning
- Remote lock and wipe
Enhanced Web Access Management

- Proxy web applications to provide authentication, authorisation, device inspection
Simplifying VDI

- Simplify virtual deployment, with no additional clients needed
- Improve scale and reliability
- Provide better user experience + SSO
- Enable vendor agnostic
## Recent News About Remote/Mobile Access

### LightReading

Juniper has sold its Junos Pulse mobile security portfolio for $250 million to Siris Capital, noting that this is consistent with its strategy to focus on “where its customers and the market is heading with High-IQ networks and building the next-generation of clouds.”

### SC Magazine

Taking advantage of a Cisco ASA Clientless SSL VPN Information Disclosure and DoS vulnerability could result in disclosure of internal information or, in certain circumstances, a reload of the affected system.

### CBR

Recently published research has found that a quarter of employees breach the company's security guidelines to remote working, putting the confidential business data at risk.

### MarketWatch

Siris Capital announced that it has completed its acquisition of the Junos Pulse business from Juniper Networks, the industry leader in network innovation, and incorporated that business under the name Pulse Secure.
Migration Strategy

• Simplify the migration of a legacy access control product to a new access control and management environment

• Consider and complete the following tasks:
  • Migration planning
  • Architectural and technology review
  • Initial platform setup and configuration
  • Configuration migration and testing
Deep Technical Migration Expertise is Needed

- Leverage best practices to mitigate migration risks
- Accelerate deployment with skilled resources that know both technologies
- Optimize availability, performance, and reliability
- Extend your staff’s reach and skills
- Capitalize quickly on enhanced functionality provided by the ADC
Transitioning from Legacy Access Products to Emerging Access Solutions

✓ Seek vendor programs that will compensate you for trading up from your outdated, legacy access control products

✓ Upgrade your existing access control products with a solution that also supports identity federation/SSO, integrated secure cloud-based access, web access management, secure mobile access

✓ Choose a solution that is flexible, extensible, and highly scalable

✓ Select vendors and partners that will deliver and implement a comprehensive migration strategy, including technical expertise
Identity and Access Management (IAM) Solution
Adaptive authentication, authorization, and access to all applications
Solutions for an Application World.